BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of the Wireline Competition Bureau's Invitation for Comment on Caller ID Authentication Best Practices Document	)))	WC Docket No. 20-324

Comments of Noble Systems Corporation

Filed October 16, 2020

Karl Koster
Noble Systems Corporation
1200 Ashwood Parkway
Atlanta, GA 30338

Chief Intellectual Property and Regulatory Counsel

I. Introduction

Noble Systems provides these comments in response to the request from the Wireline Competition Bureau (Bureau) seeking comments on the North American Numbering Council (NANC) Report recommending best practices related to caller ID authentication, i.e., *Best Practices for the Implementation of Call Authentication Frameworks* (*"Best Practices"*). Noble Systems supports the release by the Commission of the *Best Practices* document, subject to the comments below.

II. The Best Practices Document is Largely Beneficial But Its Recommendations Should Not Be Mandated

The primary source of call authentication information to date has been the various ATIS STIR/SHAKEN documents.[1] These documents are technical in nature, and do not necessarily address the various nuances and processes necessary for the service provider to support the operation the call authentication protocol. Thus, there is value in making available such explanatory resources, such as the *Best Practices* document, that provides supplemental contextual information. For example, there are various optional processes or expectations service providers are expected to perform associated with call authentication that are not defined by the standards documents and are not readily described elsewhere. Thus, releasing the *Best Practices* document to the public conveys useful information to various stakeholders regarding call authentication.

However, the *Best Practices* document acknowledges that the practices it identifies "are considered voluntary and do not imply mandatory implementation, nor should they be mandated, to ensure carriers have the flexibility and speed to respond to evolving issues."[2] Because the *Best Practices* document was written with the expectation that its recommendations would not be mandated, it would be inappropriate for the Commission to formally adopt these as mandates sometime in the future. As noted in the *Best Practices,* the practices defined "Should not be assumed to apply in all situations or to all industry types."[3] With this limitation and understanding, there is utility in the Commission releasing the *Best Practices* document.

[1] See, e.g., ATIS -1000074, ATIS-1000084, et al.
[2] *Best Practices,* Section 1, page 4.
[3] Id.

III. Flexibility Is Appropriate

The report recognizes that "VSPs [voice service providers] should have the discretion to develop their own subscriber vetting program."[4] This is particularly appropriate with respect to service providers vetting their wholesale or enterprise customers/subscribers. Various approaches may be employed by a service provider, some of which may or not be suitable or optimal for other service providers.

It is further appropriate to acknowledge flexibility is necessary for allowing how originating service providers ("OSP") should assign "A" level attestation. In instances where the OSP assigned the telephone number to the end-user originating the call, the very presence of that number on a call is sufficient to assign an "A" level attestation. In other cases, where the OSP has not provided the number (e.g., the customer is using a 'leased' number obtained from another provider), flexibility is appropriate for how the OSP determines the proper attestation level.

In certain cases, it should be acceptable for the OSP to rely upon contractual representations from its customer that it is authorized to use the telephone number in order to receive an "A" level of attestation from the OSP. To the degree the OSP determines a level of risk may be involved, there may be a spectrum of requirements placed on the customer to demonstrate they are authorized to use the telephone number. For example, the caller may be required to provide letters of authorization from the assignee of the telephone number, demonstrating that the caller is authorized to use that telephone number. Alternatively, the OSP could confirm this authorization from the original assignee of the number or employ a third-party vendor to ascertain this authorization. The OSP may require a bond or deposit to reflect a level of risk in originating calls with an "A" level of attestation. There are various approaches an OSP may avail themselves of to reduce the risk of incorrectly providing an "A" level of attestation on such calls. However, no single approach may be optimal for all OSPs.

[4] Best Practices, page 10.

IV. The *Best Practices* Description of TN Validation Requires Clarification

The *Best Practices* Document states that "Telephone Number (TN) Validation refers to the confirmation of the End-User's right-to-use the telephone number. TN Validation is necessary and appropriate when an End-User's right-to-use-the telephone number is unknown to the OSP responsible for performing SHAKEN attestation for the call."[5] There is tension between this statement that assumes TN Validation must be performed (i.e., "TN Validation is necessary") and the very definition of "B" or "C" attestation levels. Specifically, the *Best Practices* document states that "Originating Service Providers should only authenticate calls with attestation level B or C for calls where TN Validation has not been performed on the originating telephone number."[6]

An originating service provider may be unable to validate a TN from a customer originating a call. In the case of calls received at a gateway, all calls can be allocated a "C" level attestation without the service provider even attempting to perform validation. In fact, how would the service provider be expected to perform TN validation at a gateway?

In another example, a voice service provider may be receiving calls from its customer, wherein the customer exclusively originates calls using 'leased numbers' obtained elsewhere. In such cases, the originating service provider may accurately and properly assign a "B" level attestation to each call without performing any validation on the number. In fact, the originating service provider may not even attempt to validate the TN from their customer in such cases and simply (and properly) assign a "B" level attestation. Stated another way, in such instances the originating service provider may attempt and fail to validate the number (in which case a "B" level attestation is correct) or may not even attempt to validate the number (in which case, again, a "B" level attestation is correct).

Similarly, the implication that "Originating Service Providers should use a third-party validation service when they cannot or chose not to independently perform TN Validation" is misleading.[7] It also implies that TN Validation must occur, and if not performed by the OSP then it should be performed by a third-party validation service. Failing to perform TN Validation or

[5] *Best Practices,* page 12.
[6] *Best Practices,* page 5.
[7] Id.

employing a third-party validation service where the call receives a "B" or "C" level attestation is not necessarily a deficiency on the part of the originating service provider. The *Best Practices* document should consistently reflect that perspective.

V. Robocall Mitigation Is Separate from Call Authentication

Call authentication (i.e., STIR/SHAKEN) is a technology for identifying unauthorized use of a calling party number. While call authentication can be broadly described as a tool for mitigating robocalls, the phrase "robocall mitigation" is now understood to be separate and distinct from STIR/SHAKEN implementation. This understanding is borne out in light of the TRACED Act's mandate and the Commission's proposed regulations that require a covered service provider implement a robocall mitigation program if they are exempted from STIR/SHAKEN implementation. Consequently, there is a clear understanding that implementing call authentication is distinct from implementing a "robocall mitigation program."

The TRACED Act requires that "the Commission shall issue best practices that providers of voice service may use as part of the implementation of effective call authentication frameworks under paragraph (1) to take steps to ensure the calling party is accurately identified."[8] Obviously, identifying the calling party is intimately associated with call authentication, but implementing a call authentication framework is distinct from implementing a robocall mitigation program. Consequently, the discussion of "Robust robocall mitigation practices" in Section 3.6.2 of the *Best Practices* document appears outside the scope of the purpose of the document, which is to ensure that the calling party is accurately identified for implementation of an effective call authentication framework.

For example, Section 3.6.2 of *Best Practices* discusses network monitoring for suspicious robocalling patterns. It is quite feasible that gateway traffic allocated with a "C" level attestation by a service provider may (or may not) have suspicious calling patterns. However, whether the service provider receiving such calls can identify suspicious calling patterns is independent from whether the service provider can identify the calling party. Similarly, an originating service provider may know the customer for "B" level calls that originate, but the end-user behind the

[8] Traced Act, Section 4(b)(7).

customer is not known. Knowing the traffic patterns of such calls does not aid (nor hinder) the service provider with knowing the identity of the end-user or customer. In summary, it is not readily clear how monitoring the traffic patterns of such calls facilitates a service provider identifying the calling party. This demonstrates that the discussion of robocall calling patterns is separate from call authentication and the identification of the calling party.

These comments should not be interpreted as denigrating the value of publishing best practices for monitoring and investigating suspicious calls. There is value in defining such aspects, along with other best practices for reducing and investigating suspicious/illegal calls that are separate from call authentication. For example, it may be useful to document which particular traffic characteristics could be monitored to identify suspicious calls, how a service provider can cooperate with the Industry Traceback Group to investigate suspicious calls, etc. However, these actions are not directly related to the scope/purpose of the document requested by the TRACED Act, which is to ensure that the calling party is accurately identified for call authentication purposes. While Section 3.6.2 may be useful in another type of "best practices" document which the Commission may seek to release, this information does not seem germane to the TRACED Act's mandate for this document.

VI. Conclusion

There is utility in the Commission releasing a document identifying the best practices associated with call authentication. However, such best practices should be limited in addressing call authentication aspects and should not address issues outside the scope of call authentication. In summary, the current *Best Practices* document should be edited to reflect consistency with respect to whether telephone number validation must be performed and Section 3.6.2 should be excised.

Respectfully submitted on October 16, 2020

Karl Koster
Chief Intellectual Property and Regulatory Counsel,
Noble Systems Corporation
1200 Ashwood Parkway
Atlanta, GA 30338
(404) 851-1331 (x1397)
kkoster@noblesystems.com